PATENT APPLICATION

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to the Patent and Trademark Office Fax No. (571) 273-8300

on 12/26/2006 (Date) Jeannette M. Walder

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of

William D. Evans _

Application No.: 09/766,142

Filed: 01/19/2001

For: **SECURE CONTENT OBJECTS**

Examiner: Hoffman, Brandon S.

Docket No.: D/A0A87

BRIEF ON APPEAL

Appeal from Group 2136

Xerox Corporation
Jeannette M. Walder
Santa Ana, California
Telephone: (714) 565-1700
Attorney for Appellants

RECEIVED
CENTRAL FAX CENTER
DEC 2 6 2006

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest for this appeal and the present application is Xerox Corporation, by way of an Assignment recorded in the U.S. Patent and Trademark Office at Reel 11524, Frame 420-421.

II. STATEMENT OF RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, interferences or judicial proceedings, known to Appellant, Appellant's representative, or the Assignee, that may be related to, or which will directly affect or be directly affected by or have a bearing upon the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 15-29, 35, 37, 38, 41 and 42 are on appeal.

Claims 15-29, 35, 37, 38, 41 and 42 are pending.

Claims 15-29, 35, 37, 38, 41 and 42 are rejected.

Claims 1-14, 30-34, 36, 39 are canceled.

III. STATUS OF AMENDMENTS

No Amendment after Final Rejection has been filed.

IV. SUMMARY OF CLAIMED SUBJECT MATTER

The invention of claim 15 is directed to a secure content object (patent application [hereinafter "pa"] page 7, line 2 and Figure 1, element 100) for distributing and controlling access to a document and annotations associated with the document, comprising: an electronic document 12, the electronic document having been encrypted with a document encryption key, wherein access to the electronic document is available to a first set of authorized users (pa page 3, lines 5-10); an encrypted header comprising information pertaining to the electronic document (pa page 3, line 12); a first multi-key encryption table (page 3, line 7) for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key component associated with each authorized user in the first set and a plurality of dummy encryption components (page 8, lines 8), wherein the multi-key encryption table includes no information that may identify a user or the electronic document (page 4, line 27); a plurality of annotations (page 5, line 26) associated with the electronic document, generated by an annotation author and having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations (page 6, lines 1-14); a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user (page 27, lines 14-16); and a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the first multi-key encryption key table to decrypt the encrypted header, and for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation, wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and the user is an authorized annotation user; and upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document (page 3, lines 18-26; page 5, lines 20-24).

The invention of claim 35 is directed to a method for creating a secure content object for distributing and controlling access to a document and annotations associated with the document, comprising: providing an electronic document, wherein access to the electronic document is available to a first set of users (page 37, lines 16-18); responsive to a first user from the first set of users, generating a plurality of annotations pertaining to the electronic document using the document language and associating the plurality of annotations with the first user (page 37, lines 19-20); designating which users in the first set of users are authorized users have access to the plurality of annotations (page 26, lines 1-8); encrypting each annotation using an annotation encryption key associated with the first user generating the particular annotation, wherein access to an encrypted annotation is available to authorized users having access to the respective annotation encryption key; for each annotation encryption key: generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each authorized user having been designated by the first user as having access to the annotation; providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation (page 27, lines 14-16); wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found (page 3, lines 18-26; page 5, lines 20-24); concatenating the plurality of encrypted annotations in a second electronic document (page 37,lines 24-25); and merging the second electronic document and the encrypted electronic document into a third electronic document (page 38, lines 1-2) such that access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users (page 37, line 27-29).

V. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review:

1) Claims 15-29, 35, 37, 38, 41 and 42 are rejected as having been unpatentable under 35 U.S.C. §103(a) over Carter (US Patent No. 5,787,175) in view of Follendore III (US Patent No. 6,011,847) and further in view of Saito (US Patent No. 5,740,246).

VI. ARGUMENT

Appellant's secure content object and method provides a means of distributing and controlling access to a document and any annotations associated with the document. The secure content object may be used in those instances when multiple authors may wish to make annotations or comments to a common electronic document and control access (and knowledge of) their annotations among other users. For example, the original electronic document may have no restrictions on viewing (all users may view it), so it is not encrypted. One or more users/authors (including the original author) may wish to make annotations or comments to the electronic document. Each annotation author may wish to limit access to one or more of the annotations. Each such annotation may be encrypted and access limited to certain users. When an authorized user inputs its user authorization information, only those portions of the document and any authorized annotations are displayed. The user sees, in the clear, only those portions of the document to which it has access. For example, in a group of three users who share an electronic document such as a PDF file, User One can annotate the existing electronic document and grant to User Two the right to view the annotations but withhold that right from User Three. Thus User Three will be able to view the existing electronic document but will not be able to access the contents of User One's annotations in the shared file without breaking the encryption to User One's annotations.

A. Claims 15-29, 35, 37, 38, 41 and 42 are patentable under 35 U.S.C. §103(a) over Carter (US Patent No. 5,787,175) in view of Follendore III (US Patent No. 6,011,847) and further in view of Saito (US Patent No. 5,740,246).

1. Carter does not teach that "access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations."

Carter describes a method and apparatus for controlling collaborative access to a work group document. Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot. See abstract. Carter does not recognize the concept of encrypting annotations to a document separately from the document. Nor does Carter recognize that individuals within a work group may wish to

restrict access to that individual's comments to a subset of the work group. According to Carter, if a user is a member of the work group, the user has access to the entire document.

Appellant's secure content object and method of creating a secure content object enables a first set of users to have access to the document itself. Appellant's secure content object and method of creating a secure content object also enables an annotation author to determine which users within the first set may have access to which of the annotation author's annotations. In this way, sensitive comments may be restricted from certain members of the "work group".

2. Follendore III does not teach that "access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations."

Follendore III describes a system that generates encrypted labels for attachment to a message as a header or trailer thereof. See col. 1, lines 22-25. Follendore III does not recognize the concept of encrypting annotations to a document separately from the document. Nor does Follendore III recognize that individuals within a work group may wish to restrict access to that individual's comments to a subset of the work group.

Appellant's secure content object and method of creating a secure content object enables a first set of users to have access to the document itself. Appellant's secure content object and method of creating a secure content object also enables an annotation author to determine which users within the first set may have access to which of the annotation author's annotations. In this way, sensitive comments may be restricted from certain members of the "work group".

3. Saito does not teach that "access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations." Saito does not teach the concept of different users having access rights to only portions of document (annotations). At most Saito's copyright management system uses a different crypt key to encrypt an edited document.

Saito's copyright management system allows users to edit the data they receive, and to store and encrypt the edited data to others. In the case where new data is produced by editing a plurality of encrypted data which are obtained from the database and is encrypted to be supplied

to others, the crypt key for a plurality of data which are original materials and edit program as editing process with a digital signature are used as a use permit key. See Saito col. 12, lines 42-47. This is similar to the process for transferring data from the first user to a second user as described above. The only difference is that the crypt key for the edited material is different (it is not the second crypt key). Arguably, the reason for using a different crypt key based on the edit program with a digital signature to encrypt the edited data is so the second user knows that the original data has been edited. Any user who receives the edited data receives all of the edited data.

4. Saito does not provide any means for ensuring that the second user is an authorized user; any recipient of the data that has been encrypted by the first user can receive a decryption key from Saito's copyright management system.

Indeed, any user who receives the encrypted (with the first user's information) edited data is able to decrypt all of the edited data (not just a portion of it). Saito's copyright management system does not allow the first user to restrict access to particular second users. The only way the first user can control access to the encrypted edited data (or even original data) is to hope that the second user who receives the encrypted data will not further distribute the encrypted edited data. Nor does Saito's system allow a user to restrict access to portions of the document to subsequent users. Saito's copyright management system does not check to see if the second user is authorized by the first user; the copyright management system only checks to see if the first user/author's information is contained in the encrypted data. If it is, Saito's system will allow the second user (whether truly authorized or not) to receive the appropriate decryption keys to decrypt the data. Appellant's secure content object includes "a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user".

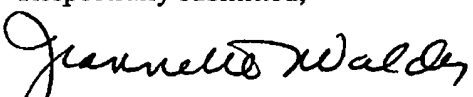
In contrast, with Appellant's secure content object, the secure content object can be lost to unauthorized users, none of whom will be able to decrypt any portion of the encrypted data. Any one can receive a secure content object with encrypted data; only people who have been authorized by the annotation author as evidenced by "a first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table

comprising at least one multi-key component associated with each authorized user in the first set" have access to the annotations.

VII. CONCLUSION

For all of the reasons discussed above, it is respectfully submitted that the rejections are in error and that claims 15-29, 35, 37, 38, 41 and 42 are in condition for allowance. For all of the above reasons, Appellants respectfully request this Honorable Board to reverse the rejections of claims 15-29, 35, 37, 38, 41 and 42.

Respectfully submitted,



Jeannette M. Walder
Registration No. 30,698

Xerox Corporation
Santa Ana, CA
Telephone: (714) 565-1700

Filed: December 26, 2006

CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL:

Claims 1 - 14 (Canceled).

15. (Previously Amended) A secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

an electronic document, the electronic document having been encrypted with a document encryption key, wherein access to the electronic document is available to a first set of authorized users;

an encrypted header comprising information pertaining to the electronic document;

a first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key component associated with each authorized user in the first set and a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user or the electronic document;

a plurality of annotations associated with the electronic document, generated by an annotation author and having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations;

a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user; and

a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the first multi-key encryption key table to decrypt the encrypted header, and for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation,

wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and the user is an authorized annotation user; and upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document.

16. (Original) The secure content object of claim 15, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

17. (Original) The secure content object of claim 15, wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules.

18. (Original) The secure content object of claim 15, wherein the user interface device comprises a second electronic document.

19. (Original) The secure content object of claim 15, wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted.

20. (Original) The secure content object of claim 15, wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and wherein the multi-key encryption table includes at least one multi-key component for each encryption key.

21. (Original) The secure content object of claim 15, wherein the encrypted header further comprises a fingerprint for identifying a predefined aspect of the electronic document.

22. (Original) The secure content object of claim 15, wherein the electronic document comprises a plurality of individual electronic documents, the encrypted header comprises information pertaining to each of the individual electronic documents.

23. (Original) The secure content object of claim 22, wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted.

24. (Original) The secure content object of claim 17, wherein the content information is selected from the group consisting of text, graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format.

25. (Previously Presented) The secure content object of claim 17, wherein the object language comprises Adobe Acrobat.

26. (Previously Presented) The secure content object of claim 17, wherein the object language comprises a language which interprets Microsoft Word documents.

27. (Original) The secure content object of claim 20, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found; and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

28. (Original) The secure content object of claim 15, wherein the electronic document includes a document ID and wherein the document encryption key includes a

combination of the document ID, the user information and the multi-key component, for each authorized user.

29. (Original) The secure content object of claim 15, wherein the electronic document comprises a first electronic document and an annotation associated therewith, wherein the annotation is encrypted using an encryption key associated with a user generating the annotation; and wherein the encrypted header includes information pertaining to the first electronic document and the annotation.

30 - 34. (Canceled).

35. (Previously Amended) A method for creating a secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

providing an electronic document, wherein access to the electronic document is available to a first set of users;

responsive to a first user from the first set of users, generating a plurality of annotations pertaining to the electronic document using the document language and associating the plurality of annotations with the first user;

designating which users in the first set of users are authorized users have access to the plurality of annotations;

encrypting each annotation using an annotation encryption key associated with the first user generating the particular annotation, wherein access to an encrypted annotation is available to authorized users having access to the respective annotation encryption key;

for each annotation encryption key:

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each authorized user having been designated by the first user as having access to the annotation;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation;

wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found;

concatenating the plurality of encrypted annotations in a second electronic document; and

merging the second electronic document and the encrypted electronic document into a third electronic document such that access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users.

36. (Canceled).

37. (Previously Presented) The method of claim 35, further comprising the step of encrypting the first electronic document using a document encryption key, wherein access to the encrypted electronic document is provided only to the first set of users;

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each of the first set of users;

generating an encrypted header comprising information pertaining to the electronic document;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of the encrypted document;

combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header; wherein valid decryption of the encrypted header indicates the document encryption key has been found.

38. (Original) The method of claim 35, further comprising adding an unencrypted header identifying the generating user to each encrypted annotation.

39. (Canceled).

40. (Canceled).

41. (Previously Presented) The method of claim 35, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the annotation encryption key has been found.

42. (Original) The method of claim 35, wherein the separate file and the electronic document are stored in different locations.

EVIDENCE APPENDIX

NONE

RELATED PROCEEDINGS APPENDIX

NONE